VLAN Zuweisung und WLAN Registrierung über Zertifikate bzw. Nutzername mit NPS RADIUS Windows Server

Inhaltsverzeichnis

Hallo zusammen.

Ich habe mir aus Folgendes eingerichtet. Es sorgt für Sicherheit und weniger Administrationsaufwand (kein neu Konfigurieren einzelner Switchports etc.). Ich will das hier mal für die Nachwelt festhalten (und damit ich es selbst wieder vergessen kann).

Was wollte ich erreichen?

1. Nutzer sollen sich mit ihrem AD-Nutzernamen am WLAN anmelden können.

2. Clients der Active-Directory sollen direkt in VLAN x verschoben werden, wenn sie sich im WLAN anmelden oder an einem Switch eingesteckt werden (Port unabhängig). Das geht ohne Nutzereingabe, sondern über Zertifikate.

3. nur noch eine SSID für alle VLANs (nur bedingt möglich, da hier die Clients mitspielen müssen. Z.B. unterstützen nicht alle IoT Geräte WPA2-Enterprise)

Voraussetzungen:

1. funktionierendes Active Directory (inkl. Benutzer/Computerverwaltung, sowie Gruppenrichtlinienverwaltung)

2. in AD registrierte Zertifizierungsstelle (Rolle unter Windows Server)

3. in AD registrierter NPS (Network Policy Server - deutsch: Netzwerkrichtlinienserver [Rolle unter Windows Server]) auch als RADIUS bekannt.

Wie ihr das alles trennt, ist letztendlich euer eigenes Ding, da es hier auf Sicherheit, Performance usw. ankommt.

Ich finde es immer schwierig, wo ich bei solchen Tutorials anfangen soll. Jedoch habe ich entschlossen, auf die grundlegende Einrichtung vom NPS und der CA zu verzichten. Hierzu gibt es genügend (gute) Tutorials im Netz. Ich gehe also davon aus, dass dies zum Zeitpunkt des Weiterlesens erfolgt und die Zusammenhänge verstanden sind.

Meine Infrastruktur sieht wie folgt aus. Das ist keine Vorgabe, ich zeige das nur, damit ihr die Namen der Server (falls relevant) bzw. die Rollenverteilung seht. Ich hoffe hiermit das ein oder andere Fragezeichen vermeiden zu können.

DC1: Active Directory Verwaltungsdienste. Für das Tutorial relevant sind nur die Benutzer/Computerverwaltung und die Gruppenrichtlinienverwaltung.

Util-01: allgemeiner Anwendungsserver. Hier läuft der NPS (Netzwerkrichtlinienserver).

CA-01: Certificat-Authority. Hier sind die AD-Zertifikatsdienste installiert.

Ich arbeite mit Windows Server 2019 und Windows 11 Clients.

Getestet habe ich das Ganze auch mit Win Server 2016 und Windows 10 Clients.

Laut Internet sollte die Prozedur ab Windows Server 2012 (R2?) und Windows 7 (Vista?) Clients funktionieren.

1 Anlegen der Windowsgruppen

AD Nutzer und Computerverwaltung öffnen und Gruppen anlegen, welche sich am RADIUS authentifizieren dürfen.

Grp-LanDevices (Alle AD Clients, welche sich per LAN verbinden, ihr müsst also Computer angeben, keine Benutzer)

Grp-WLanDevices (Alle AD Clients, welche sich per WLAN verbinden sollen, ihr müsst also Computer angeben, keine Benutzer)

Grp-WLAN-IoT (beinhaltet bei mir nur einen Nutzer, der für alle IoT Geräte verwendet wird, welche sich am WLAN anmelden)

Grp-WLAN-AD-Home (beinhaltet alle in AD angelegten Nutzer, welche sich mit ihrem Nutzernamen am WLAN anmelden können sollen)

2 Gruppenrichtlinien erstellen

Es gibt zwei GPOs, die ich für mein Vorhaben verwende.

Die GPO "Zertifikatsverteilung" ist für die automatische Zertifikatsverteilung verantwortlich. Sie wirkt auf alle Clients.

Die GPO "Wlan Profil" ist für die Verteilung des WLAN-Profils verantwortlich. Sie wirkt nur auf Clients, welche auch WLAN nutzen.

GPO "Zertifikatsverteilung"

Computerkonfiguration - Richtlinien - Windows-Einstellungen - Sicherheitseinstellungen - Richtlinien für öffentliche Schlüssel - Einstellungen der automatischen Zertifikatsanforderung

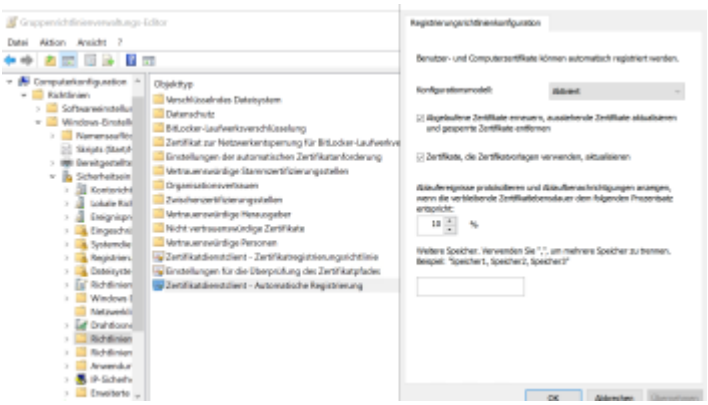
Rechtsklick - neu - Automatische Zertifikatsanforderung

Assistent durchklicken und "Computer" auswählen. Fertigstellen.

ubiquiti-networks-forum.de/attachment/15320/

Computerkonfiguration - Richtlinien - Windows-Einstellungen - Sicherheitseinstellungen - Richtlinien für öffentliche Schlüssel

Doppelklick "Zertifikatdienstclient - Automatische Registrierung". "Aktiviert" auswählen und beide Haken setzen.

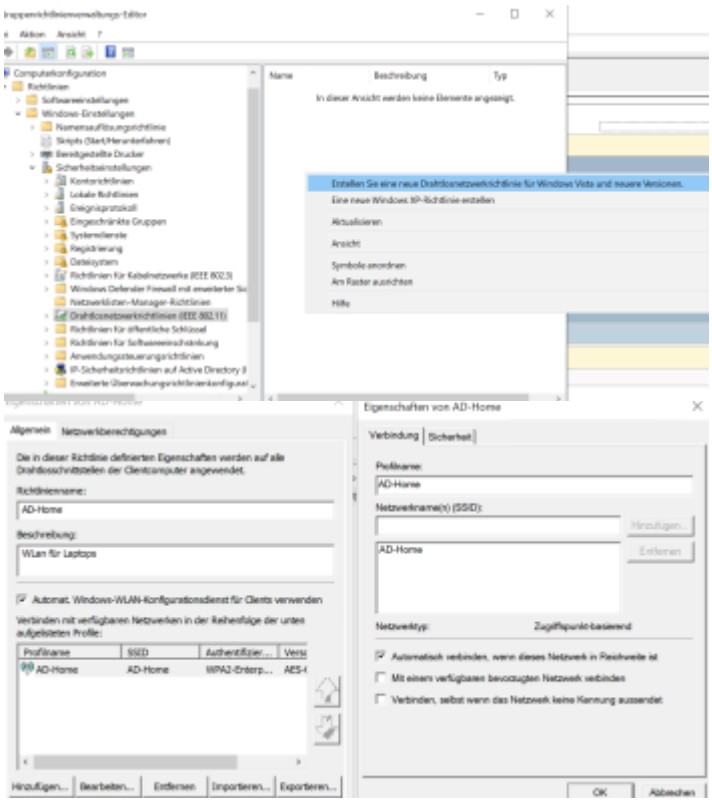


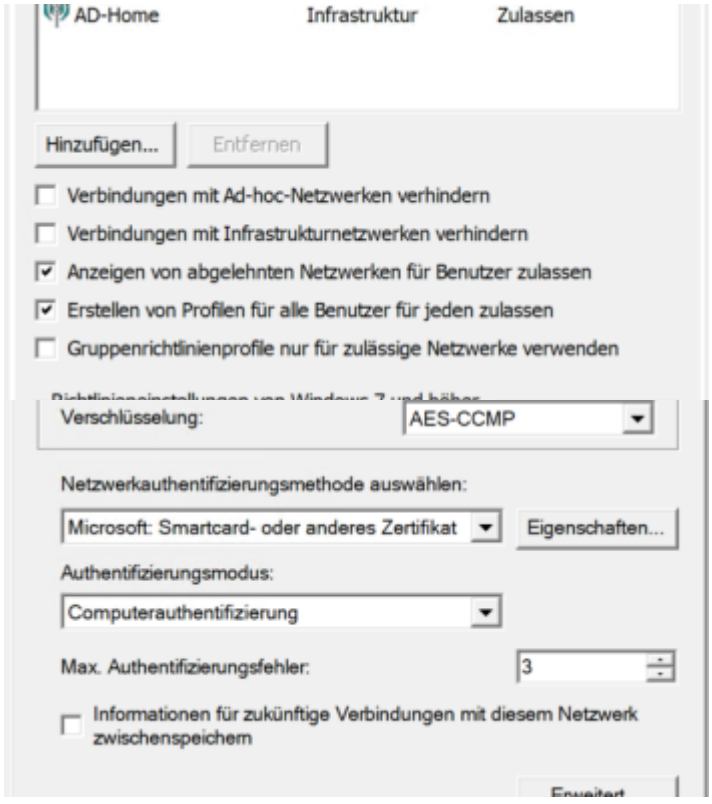
GPO "Wlan Profil"

Computerkonfiguration - Richtlinien - Windows-Einstellungen - Sicherheitseinstellungen - Drahtlosnetzerkrichtlinien

Rechtsklick - "Erstellen Sie eine neue Drahtlosnetzwerkrichtlinie für Windows Vista und neuere Versionen"

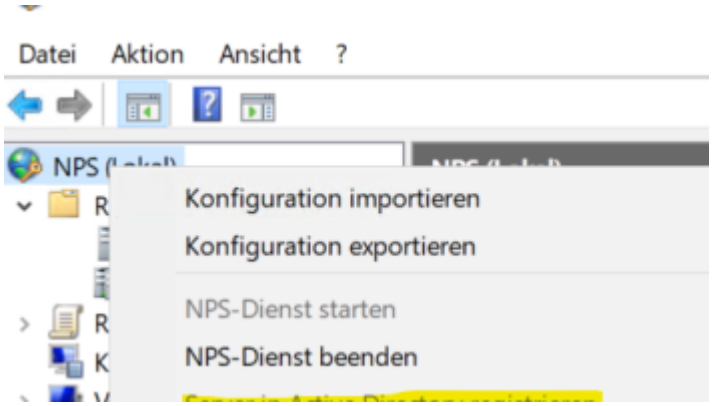
Euere SSID anlegen. Wichtig: die Schreibweise muss identisch sein. Einstellungen entnehmt ihr bitte den Screenshots.


Computerkonfiguration
Richtlinien
Softwareeinstellungen
Windows-Einstellungen
Name
Beschreibung
Typ
In dieser Ansicht werden keine Elemente angezeigt.
Erstellen Sie eine neue Drahtlosnetzwerkrichtlinie für Windows Vista und neuere Versionen.
Eine neue Windows XP-Richtlinie erstellen
Aktualisieren
Ansicht
Symbole anordnen
Am Raster ausrichten
Hilfe
Allgemein
Netzwerkberechtigungen
Die in dieser Richtlinie definierten Eigenschaften werden auf alle Drahtlosschnittstellen der Clientcomputer angewendet.
Richtliniename:
AD-Home
Beschreibung:
WLan für Laptops
Automat. Windows-WLAN-Konfigurationsdienst für Clients verwenden
Verbinden mit verfügbaren Netzwerken in der Reihenfolge der unten aufgelisteten Profile:
Profilname
SSID
Authentifizier...
Versi
AD-Home
AD-Home
WPA2-Enterp...
Hinzufügen...
Bearbeiten...
Entfernen
Importieren...
Exportieren...
Eigenschaften von AD-Home
Verbindung
Sicherheit
Profilname:
AD-Home
Netzwerkname(n) (SSID):
Hinzufügen...
Entfernen
AD-Home
Netzwerktyp:
Zugriffspunkt-basierend
Automatisch verbinden, wenn dieses Netzwerk in Reichweite ist
Mit einem verfügbaren bevorzugten Netzwerk verbinden
Verbinden, selbst wenn das Netzwerk keine Kennung aussendet
OK
Abbrechen


AD-Home
Infrastruktur
Zulassen
Hinzufügen...
Entfernen
Verbindungen mit Ad-hoc-Netzwerken verhindern
Verbindungen mit Infrastrukturnetzwerken verhindern
Anzeigen von abgelehnten Netzwerken für Benutzer zulassen
Erstellen von Profilen für alle Benutzer für jeden zulassen
Gruppenrichtlinienprofile nur für zulässige Netzwerke verwenden
Verschlüsselung:
AES-CCMP
Netzwerkauthentifizierungsmethode auswählen:
Microsoft: Smartcard- oder anderes Zertifikat
Eigenschaften...
Authentifizierungsmodus:
Computerauthentifizierung
Max. Authentifizierungsfehler:
3
Informationen für zukünftige Verbindungen mit diesem Netzwerk zwischenspeichern

3 NPS konfigurieren

Server-Manager - Tools - Netzwerkrichtlinienserver - Rechtsklick auf "NPS (lokal)" - Server in Active Directory registrieren (bei mir ausgegraut, da bereits erledigt)



Der Server, auf dem der NPS läuft, muss Mitglied der Gruppe "RAS- und IAS-Server" sein. Dann bezieht er automatisch ein Zertifikat von der Zertifizierungsstelle.

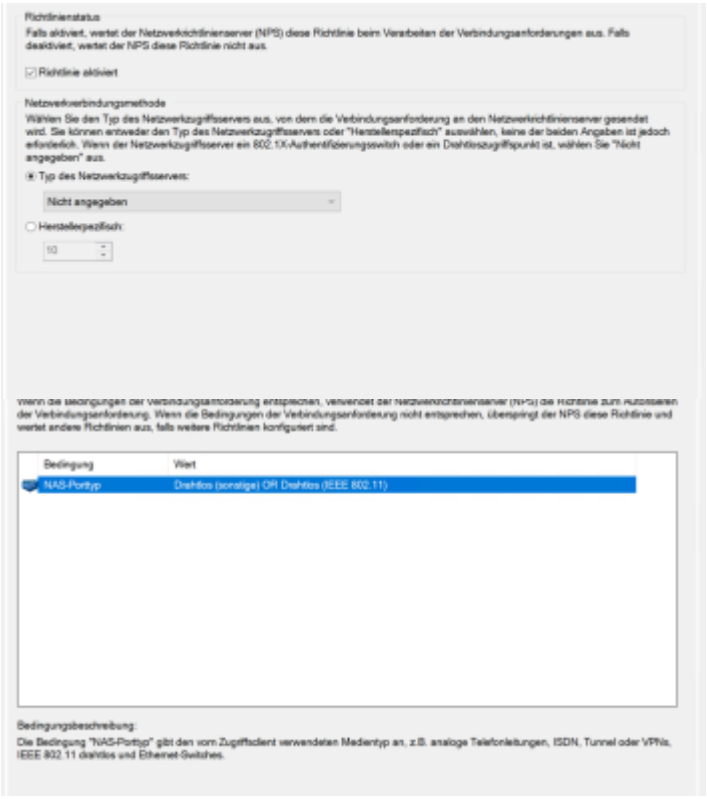
Anschließend Rechtsklick auf "RADIUS-Clients und -Server" - Neu

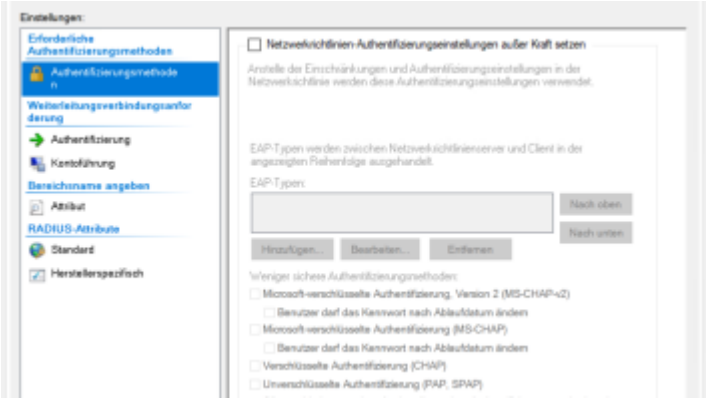
Hier legt ihr nun all eure Accesspoint und Switches an. Das ist eine Unifi-Eigenheit. andere Hersteller haben das eleganter gelöst und man muss nur den Controller anlegen. Daher kann es je nach Umfang eurer Infrastruktur einige Einträge geben. Beim Reiter "Erweitert" lasst ihr Standard im Drop-Down Menü stehen. Den "gemeinsamen Schlüssel" notiert ihr euch bitte, da dieser nach Eingabe nicht mehr angesehen werden kann. Ihr benötigt den nachher im inifi-Controller. Deswegen ist es auch zwingend nötig, bei allen angelegten Geräten im NPS den selben Schlüssel zu nehmen.

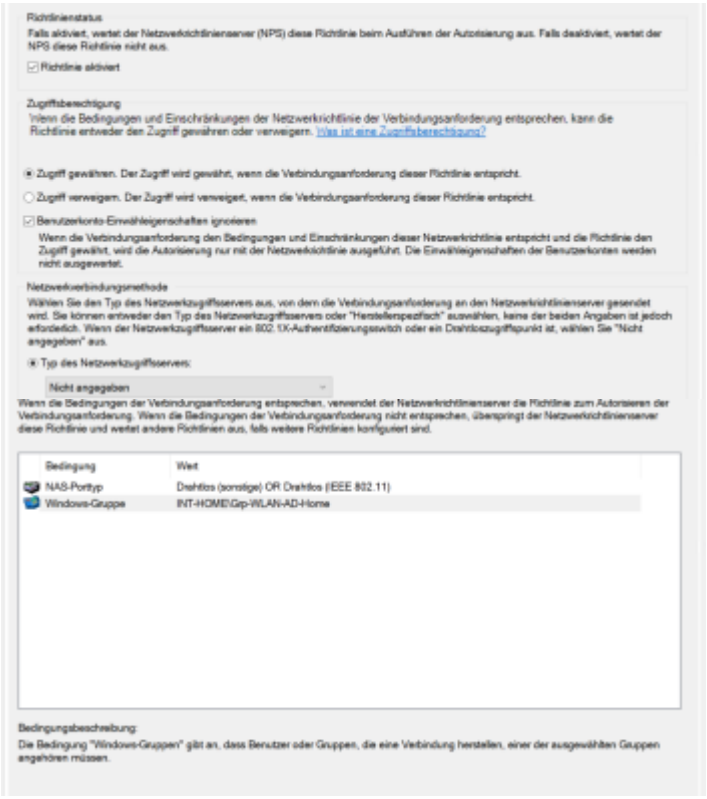
Als nächstes werden die Verbindungsanforderungsrichtlinie und die Netzwerkrichtlinie erstellt. Bei mir sind es 3 bzw. mit der Standard-Richtlinie eben dann 4.

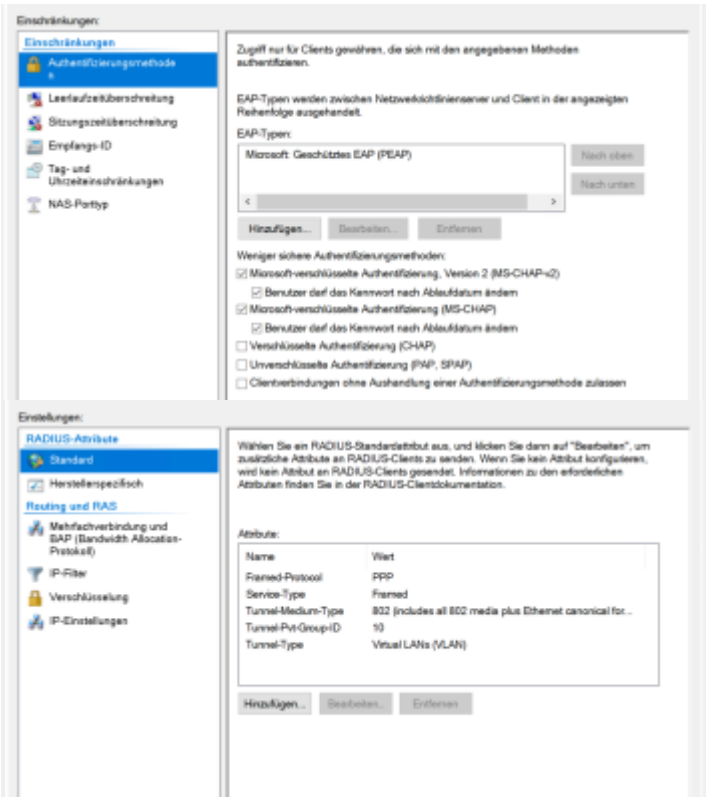
Unterschieden habe ich in Nutzer, die ins interne Netz dürfen, IoT-Nutzer und den Sonderfall mit der Zertifikat-Authentifizierung. Die ersten drei Screenshots jeweils sind die Verbindungsanforderungsrichtlinie, die vier weiteren dann die Netzwerkrichtlinie. Also wie folgt:

"Wifi User Auth AD-Home"

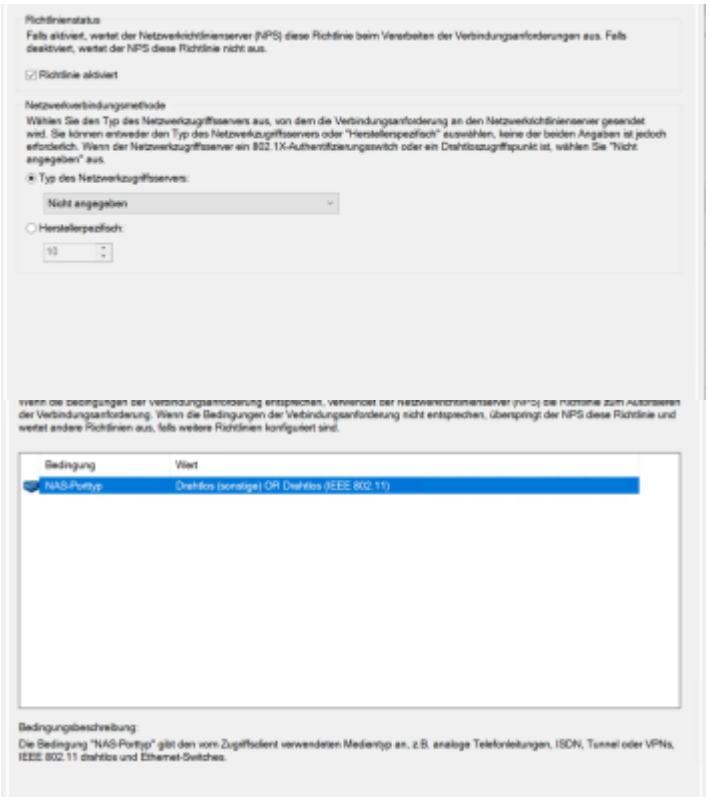

Richtlinienstatus
Falls aktiviert, wertet der Netzwerkrichtlinienserver (NPS) diese Richtlinie beim Verarbeiten der Verbindungsanforderungen aus. Falls deaktiviert, wertet der NPS diese Richtlinie nicht aus.
Richtlinie aktiviert
Netzwerkverbindungsmethode
Wählen Sie den Typ des Netzwerkzugriffsservers aus, von dem die Verbindungsanforderung an den Netzwerkrichtlinienserver gesendet wird. Sie können entweder den Typ des Netzwerkzugriffsservers oder "Herstellerspezifisch" auswählen, keine der beiden Angaben ist jedoch erforderlich. Wenn der Netzwerkzugriffsserver ein 802.1X-Authentifizierungsswitch oder ein Drahtloszugriffspunkt ist, wählen Sie "Nicht angegeben" aus.
Typ des Netzwerkzugriffsservers:
Nicht angegeben
Herstellerspezifisch:
10
der Verbindungsanforderung. Wenn die Bedingungen der Verbindungsanforderung nicht entsprechen, überspringt der NPS diese Richtlinie und wertet andere Richtlinien aus, falls weitere Richtlinien konfiguriert sind.
Bedingung
Wert
NAS-Porttyp
Drahtlos (sonstige) OR Drahtlos (IEEE 802.11)
Bedingungsbeschreibung:
Die Bedingung "NAS-Porttyp" gibt den vom Zugriffsclient verwendeten Medientyp an, z.B. analoge Telefonleitungen, ISDN, Tunnel oder VPNs, IEEE 802.11 drahtlos und Ethernet-Switches.

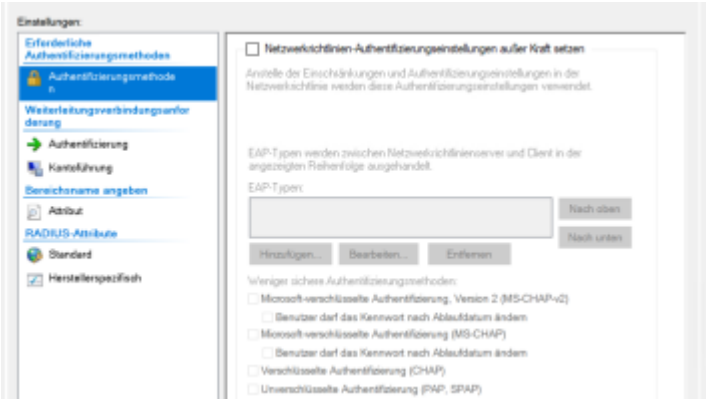

Einstellungen:
Erforderliche Authentifizierungsmethoden
Authentifizierungsmethoden
Weiterleitungsverbindungsanforderung
Authentifizierung
Kontoführung
Bereichsname angeben
Attribut
RADIUS-Attribute
Standard
Herstellerspezifisch
Netzwerkrichtlinien-Authentifizierungseinstellungen außer Kraft setzen
Anstelle der Einschränkungen und Authentifizierungseinstellungen in der Netzwerkrichtlinie werden diese Authentifizierungseinstellungen verwendet.
EAP-Typen werden zwischen Netzwerkrichtlinienserver und Client in der angezeigten Reihenfolge ausgehandelt.
EAP-Typen:
Nach oben
Nach unten
Hinzufügen...
Bearbeiten...
Entfernen
Weniger sichere Authentifizierungsmethoden:
Microsoft-verschlüsselte Authentifizierung, Version 2 (MS-CHAP-v2)
Benutzer darf das Kennwort nach Ablaufdatum ändern
Microsoft-verschlüsselte Authentifizierung (MS-CHAP)
Benutzer darf das Kennwort nach Ablaufdatum ändern
Verschlüsselte Authentifizierung (CHAP)
Unverschlüsselte Authentifizierung (PAP, SPAP)

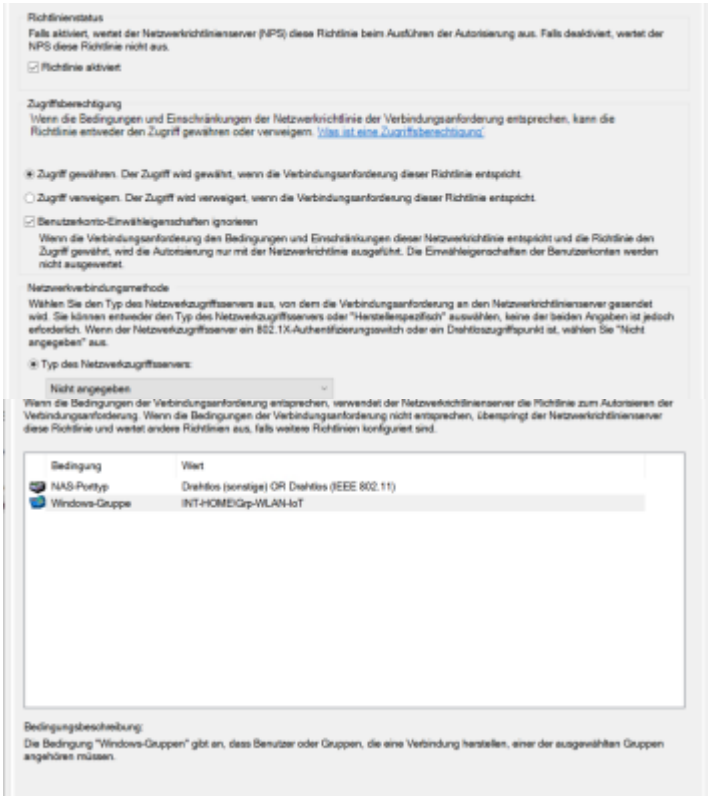

Richtlinienstatus
Falls aktiviert, wertet der Netzwerkrichtlinienserver (NPS) diese Richtlinie beim Ausführen der Autorisierung aus. Falls deaktiviert, wertet der NPS diese Richtlinie nicht aus.
Richtlinie aktiviert
Zugriffsberechtigung
Wenn die Bedingungen und Einschränkungen der Netzwerkrichtlinie der Verbindungsanforderung entsprechen, kann die Richtlinie entweder den Zugriff gewähren oder verweigern. Was ist eine Zugriffsberechtigung?
Zugriff gewähren. Der Zugriff wird gewährt, wenn die Verbindungsanforderung dieser Richtlinie entspricht.
Zugriff verweigern. Der Zugriff wird verweigert, wenn die Verbindungsanforderung dieser Richtlinie entspricht.
Benutzerkonto-Einwähleigenschaften ignorieren
Wenn die Verbindungsanforderung den Bedingungen und Einschränkungen dieser Netzwerkrichtlinie entspricht und die Richtlinie den Zugriff gewährt, wird die Autorisierung nur mit der Netzwerkrichtlinie ausgeführt. Die Einwähleigenschaften der Benutzerkonten werden nicht ausgewertet.
Netzwerkverbindungsmethode
Wählen Sie den Typ des Netzwerkzugriffsservers aus, von dem die Verbindungsanforderung an den Netzwerkrichtlinienserver gesendet wird. Sie können entweder den Typ des Netzwerkzugriffsservers oder "Herstellerspezifisch" auswählen, keine der beiden Angaben ist jedoch erforderlich. Wenn der Netzwerkzugriffsserver ein 802.1X-Authentifizierungsswitch oder ein Drahtloszugriffspunkt ist, wählen Sie "Nicht angegeben" aus.
Typ des Netzwerkzugriffsservers:
Nicht angegeben
Wenn die Bedingungen der Verbindungsanforderung entsprechen, verwendet der Netzwerkrichtlinienserver die Richtlinie zum Autorisieren der Verbindungsanforderung. Wenn die Bedingungen der Verbindungsanforderung nicht entsprechen, überspringt der Netzwerkrichtlinienserver diese Richtlinie und wertet andere Richtlinien aus, falls weitere Richtlinien konfiguriert sind.
Bedingung
Wert
NAS-Porttyp
Drahtlos (sonstige) OR Drahtlos (IEEE 802.11)
Windows-Gruppe
INT-HOME\Grp-WLAN-AD-Home
Bedingungsbeschreibung:
Die Bedingung "Windows-Gruppen" gibt an, dass Benutzer oder Gruppen, die eine Verbindung herstellen, einer der ausgewählten Gruppen angehören müssen.

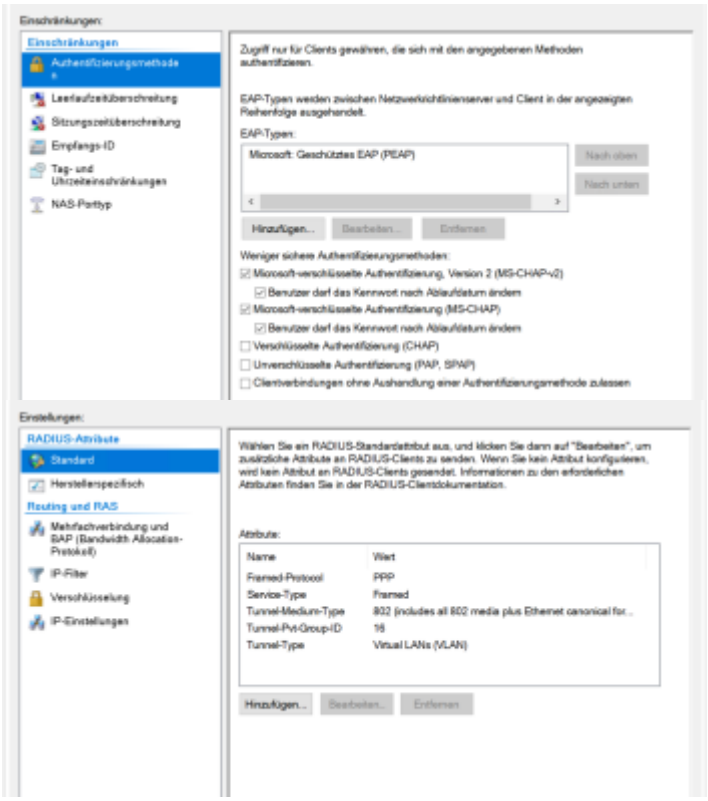

Einschränkungen:
Einschränkungen
Authentifizierungsmethode
Laufzeitüberschreitung
Sitzungszeitüberschreitung
Empfangs-ID
Tag- und Uhrzeiteinschränkungen
NAS-Porttyp
Zugriff nur für Clients gewähren, die sich mit den angegebenen Methoden authentifizieren.
EAP-Typen werden zwischen Netzwerkrichtlinienserver und Client in der angezeigten Reihenfolge ausgehandelt.
EAP-Typen:
Microsoft: Geschütztes EAP (PEAP)
Nach oben
Nach unten
Hinzufügen...
Bearbeiten...
Entfernen
Weniger sichere Authentifizierungsmethoden:
Microsoft-verschlüsselte Authentifizierung, Version 2 (MS-CHAP-v2)
Benutzer darf das Kennwort nach Ablaufdatum ändern
Microsoft-verschlüsselte Authentifizierung (MS-CHAP)
Benutzer darf das Kennwort nach Ablaufdatum ändern
Verschlüsselte Authentifizierung (CHAP)
Unverschlüsselte Authentifizierung (PAP, SPAP)
Clientverbindungen ohne Aushandlung einer Authentifizierungsmethode zulassen
Einstellungen:
RADIUS-Attribute
Standard
Herstellerspezifisch
Routing und RAS
Mehrfachverbindung und BAP (Bandwidth Allocation-Protokoll)
IP-Filter
Verschlüsselung
IP-Einstellungen
Wählen Sie ein RADIUS-Standardattribut aus, und klicken Sie dann auf "Bearbeiten", um zusätzliche Attribute an RADIUS-Clients zu senden. Wenn Sie kein Attribut konfigurieren, wird kein Attribut an RADIUS-Clients gesendet. Informationen zu den erforderlichen Attributen finden Sie in der RADIUS-Clientdokumentation.
Attribute:
Name
Wert
Framed-Protocol
PPP
Service-Type
Framed
Tunnel-Medium-Type
802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID
10
Tunnel-Type
Virtual LANs (VLAN)
Hinzufügen...
Bearbeiten...
Entfernen

"Wifi User Auth Iot"

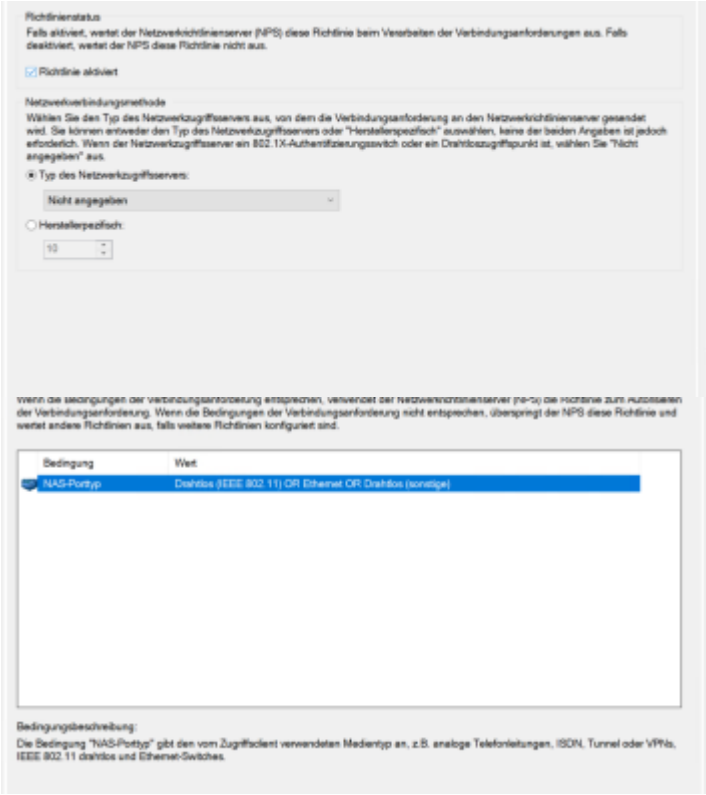


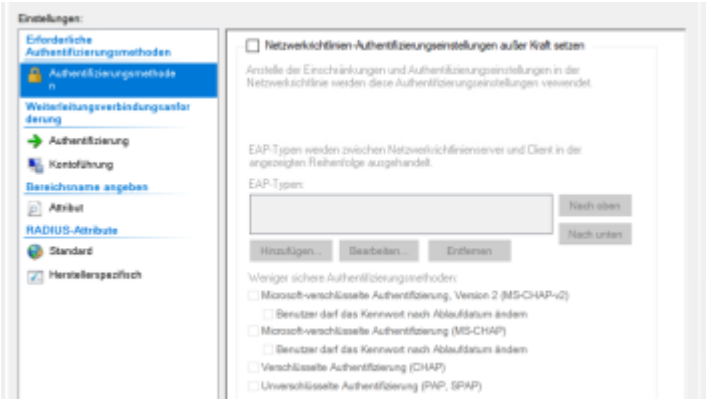


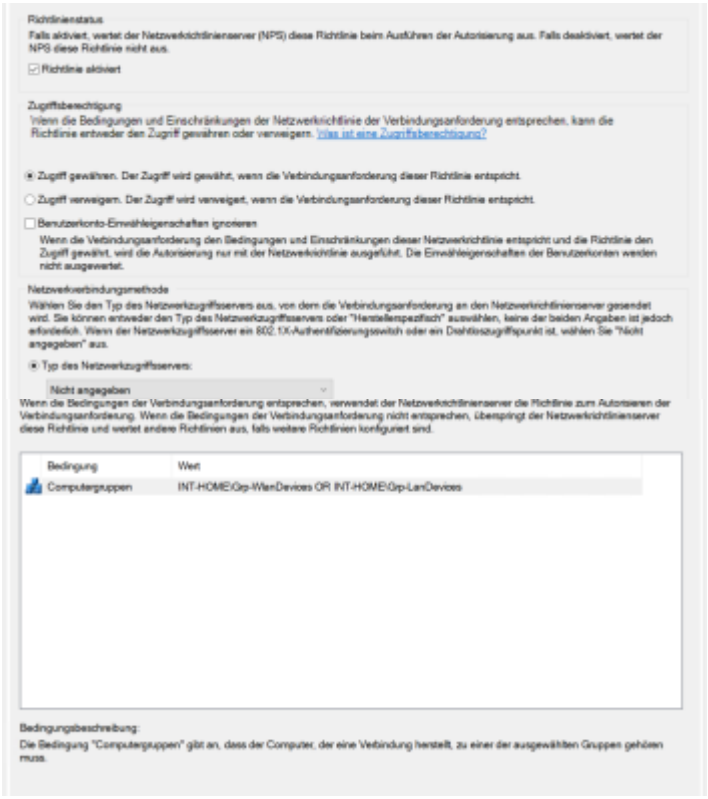

Richtlinienstatus
Falls aktiviert, wertet der Netzwerkrichtlinienserver (NPS) diese Richtlinie beim Ausführen der Autorisierung aus. Falls deaktiviert, wertet der NPS diese Richtlinie nicht aus.
Richtlinie aktiviert
Zugriffsberechtigung
Wenn die Bedingungen und Einschränkungen der Netzwerkrichtlinie der Verbindungsanforderung entsprechen, kann die Richtlinie entweder den Zugriff gewähren oder verweigern. Was ist eine Zugriffsberechtigung?
Zugriff gewähren. Der Zugriff wird gewährt, wenn die Verbindungsanforderung dieser Richtlinie entspricht.
Zugriff verweigern. Der Zugriff wird verweigert, wenn die Verbindungsanforderung dieser Richtlinie entspricht.
Benutzerkonto-Einwähleigenschaften ignorieren
Wenn die Verbindungsanforderung den Bedingungen und Einschränkungen dieser Netzwerkrichtlinie entspricht und die Richtlinie den Zugriff gewährt, wird die Autorisierung nur mit der Netzwerkrichtlinie ausgeführt. Die Einwähleigenschaften der Benutzerkonten werden nicht ausgewertet.
Netzwerkverbindungsmethode
Wählen Sie den Typ des Netzwerkzugriffsservers aus, von dem die Verbindungsanforderung an den Netzwerkrichtlinienserver gesendet wird. Sie können entweder den Typ des Netzwerkzugriffsservers oder "Herstellerspezifisch" auswählen, keine der beiden Angaben ist jedoch erforderlich. Wenn der Netzwerkzugriffsserver ein 802.1X-Authentifizierungsswitch oder ein Drahtloszugriffspunkt ist, wählen Sie "Nicht angegeben" aus.
Typ des Netzwerkzugriffsservers:
Nicht angegeben
Wenn die Bedingungen der Verbindungsanforderung entsprechen, verwendet der Netzwerkrichtlinienserver die Richtlinie zum Autorisieren der Verbindungsanforderung. Wenn die Bedingungen der Verbindungsanforderung nicht entsprechen, überspringt der Netzwerkrichtlinienserver diese Richtlinie und wertet andere Richtlinien aus, falls weitere Richtlinien konfiguriert sind.
Bedingung
Wert
NAS-Porttyp
Drahtlos (sonstige) OR Drahtlos (IEEE 802.11)
Windows-Gruppe
INT-HOME\Grp-WLAN-IoT
Bedingungsbeschreibung:
Die Bedingung "Windows-Gruppen" gibt an, dass Benutzer oder Gruppen, die eine Verbindung herstellen, einer der ausgewählten Gruppen angehören müssen.

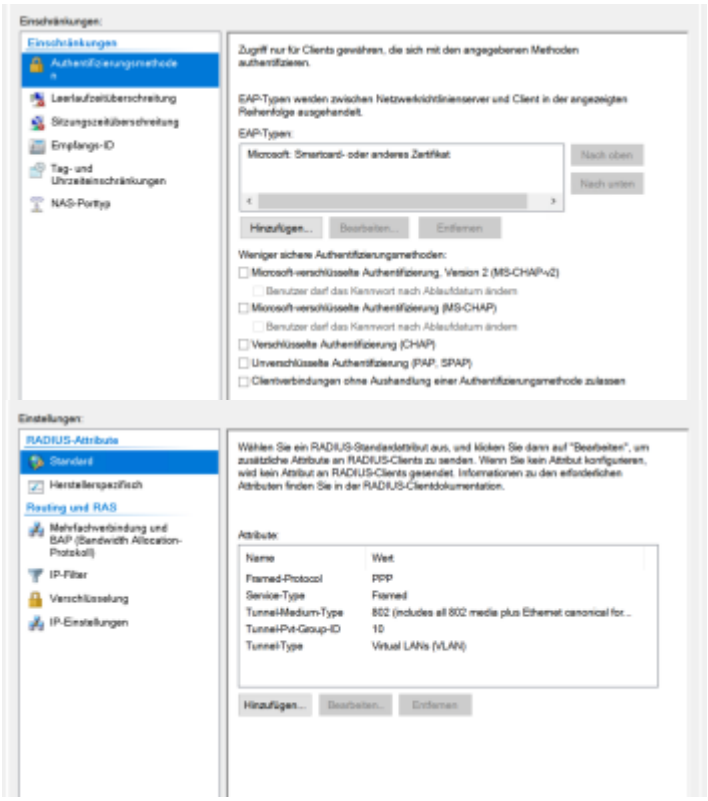

Einschränkungen:
Einschränkungen
Authentifizierungsmethode
Leerlaufzeitüberschreitung
Sitzungszeitüberschreitung
Empfangs-ID
Tag- und Uhrzeiteinschränkungen
NAS-Porttyp
Zugriff nur für Clients gewähren, die sich mit den angegebenen Methoden authentifizieren.
EAP-Typen werden zwischen Netzwerkrichtlinienserver und Client in der angezeigten Reihenfolge ausgehandelt.
EAP-Typen:
Microsoft: Geschütztes EAP (PEAP)
Nach oben
Nach unten
Hinzufügen...
Bearbeiten...
Entfernen
Weniger sichere Authentifizierungsmethoden:
Microsoft-verschlüsselte Authentifizierung, Version 2 (MS-CHAP-v2)
Benutzer darf das Kennwort nach Ablaufdatum ändern
Microsoft-verschlüsselte Authentifizierung (MS-CHAP)
Benutzer darf das Kennwort nach Ablaufdatum ändern
Verschlüsselte Authentifizierung (CHAP)
Unverschlüsselte Authentifizierung (PAP, SPAP)
Clientverbindungen ohne Aushandlung einer Authentifizierungsmethode zulassen
Einstellungen:
RADIUS-Attribute
Standard
Herstellerspezifisch
Routing und RAS
Mehrfachverbindung und BAP (Bandwidth Allocation-Protokoll)
IP-Filter
Verschlüsselung
IP-Einstellungen
Wählen Sie ein RADIUS-Standardattribut aus, und klicken Sie dann auf "Bearbeiten", um zusätzliche Attribute an RADIUS-Clients zu senden. Wenn Sie kein Attribut konfigurieren, wird kein Attribut an RADIUS-Clients gesendet. Informationen zu den erforderlichen Attributen finden Sie in der RADIUS-Clientdokumentation.
Attribute:
Name
Wert
Framed-Protocol
PPP
Service-Type
Framed
Tunnel-Medium-Type
802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID
16
Tunnel-Type
Virtual LANs (VLAN)
Hinzufügen...
Bearbeiten...
Entfernen

"Wifi Device Cert Auth"






Richtlinienstatus
Falls aktiviert, wertet der Netzwerkrichtlinienserver (NPS) diese Richtlinie beim Ausführen der Autorisierung aus. Falls deaktiviert, wertet der NPS diese Richtlinie nicht aus.
Richtlinie aktiviert
Zugriffsberechtigung
Wenn die Bedingungen und Einschränkungen der Netzwerkrichtlinie der Verbindungsanforderung entsprechen, kann die Richtlinie entweder den Zugriff gewähren oder verweigern. Was ist eine Zugriffsberechtigung?
Zugriff gewähren. Der Zugriff wird gewährt, wenn die Verbindungsanforderung dieser Richtlinie entspricht.
Zugriff verweigern. Der Zugriff wird verweigert, wenn die Verbindungsanforderung dieser Richtlinie entspricht.
Benutzerkonto-Einwähleigenschaften ignorieren
Wenn die Verbindungsanforderung den Bedingungen und Einschränkungen dieser Netzwerkrichtlinie entspricht und die Richtlinie den Zugriff gewährt, wird die Autorisierung nur mit der Netzwerkrichtlinie ausgeführt. Die Einwähleigenschaften der Benutzerkonten werden nicht ausgewertet.
Netzwerkverbindungsmethode
Wählen Sie den Typ des Netzwerkzugriffsservers aus, von dem die Verbindungsanforderung an den Netzwerkrichtlinienserver gesendet wird. Sie können entweder den Typ des Netzwerkzugriffsservers oder "Herstellerspezifisch" auswählen, keine der beiden Angaben ist jedoch erforderlich. Wenn der Netzwerkzugriffsserver ein 802.1X-Authentifizierungsswitch oder ein Drahtloszugriffspunkt ist, wählen Sie "Nicht angegeben" aus.
Typ des Netzwerkzugriffsservers:
Nicht angegeben
Wenn die Bedingungen der Verbindungsanforderung entsprechen, verwendet der Netzwerkrichtlinienserver die Richtlinie zum Autorisieren der Verbindungsanforderung. Wenn die Bedingungen der Verbindungsanforderung nicht entsprechen, überspringt der Netzwerkrichtlinienserver diese Richtlinie und wertet andere Richtlinien aus, falls weitere Richtlinien konfiguriert sind.
Bedingung
Wert
Computergruppen
INT-HOME\Grp-WlanDevices OR INT-HOME\Grp-LanDevices
Bedingungsbeschreibung:
Die Bedingung "Computergruppen" gibt an, dass der Computer, der eine Verbindung herstellt, zu einer der ausgewählten Gruppen gehören muss.


Einschränkungen:
Einschränkungen
Authentifizierungsmethode
Leerlaufzeitüberschreitung
Sitzungszeitüberschreitung
Empfangs-ID
Tag- und Uhrzeiteinschränkungen
NAS-Porttyp
Zugriff nur für Clients gewähren, die sich mit den angegebenen Methoden authentifizieren.
EAP-Typen werden zwischen Netzwerkrichtlinienserver und Client in der angezeigten Reihenfolge ausgehandelt.
EAP-Typen:
Microsoft: Smartcard- oder anderes Zertifikat
Nach oben
Nach unten
Hinzufügen...
Bearbeiten...
Entfernen
Weniger sichere Authentifizierungsmethoden:
Microsoft-verschlüsselte Authentifizierung, Version 2 (MS-CHAP-v2)
Benutzer darf das Kennwort nach Ablaufdatum ändern
Microsoft-verschlüsselte Authentifizierung (MS-CHAP)
Benutzer darf das Kennwort nach Ablaufdatum ändern
Verschlüsselte Authentifizierung (CHAP)
Unverschlüsselte Authentifizierung (PAP, SPAP)
Clientverbindungen ohne Aushandlung einer Authentifizierungsmethode zulassen
Einstellungen:
RADIUS-Attribute
Standard
Herstellerspezifisch
Routing und RAS
Mehrfachverbindung und BAP (Bandwidth Allocation-Protokoll)
IP-Filter
Verschlüsselung
IP-Einstellungen
Wählen Sie ein RADIUS-Standardattribut aus, und klicken Sie dann auf "Bearbeiten", um zusätzliche Attribute an RADIUS-Clients zu senden. Wenn Sie kein Attribut konfigurieren, wird kein Attribut an RADIUS-Clients gesendet. Informationen zu den erforderlichen Attributen finden Sie in der RADIUS-Clientdokumentation.
Attribute:
Name
Wert
Framed-Protocol
PPP
Service-Type
Framed
Tunnel-Medium-Type
802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID
10
Tunnel-Type
Virtual LANs (VLAN)
Hinzufügen...
Bearbeiten...
Entfernen

4 Konfigurieren Unifi-Controller

am Beispiel der UDM-Pro (sollte jedoch auf allen anderen Instanzen wie Cloudkey etc. sehr ähnlich funktionieren)

Wechselt zu Netzwerk - Einstellungen - Profile - RADIUS - Create New RADIUS Profile

Einstellungen wie folgt:

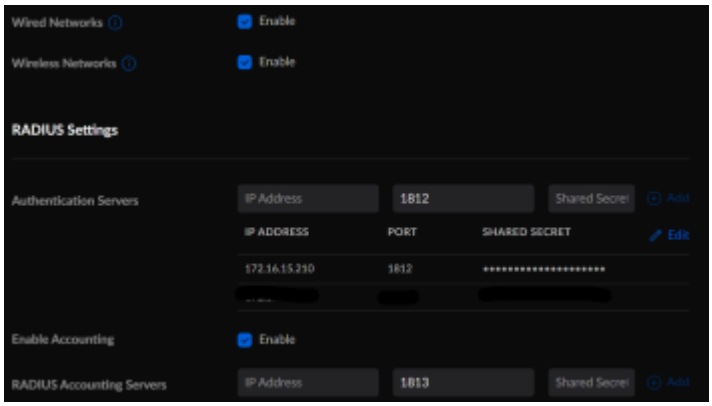
"RADIUS Assigned VLAN Support" beide Haken setzen, sowohl Wired als auch Wireless

"RADIUS Settings"

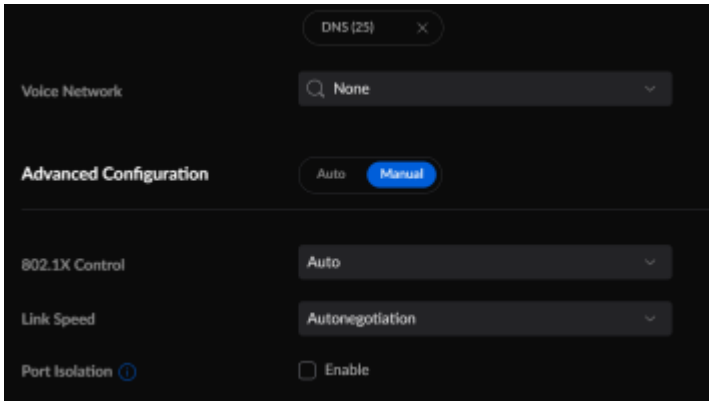
Authentication Server: IP eures NPS eingeben und auch den gemeinsamen Schlüssel aus Punkt 4. Bei Port tragt ihr Port Nummer 1812 ein.

Haken setzen bei "enable Accounting" (ist nicht erforderlich, jedoch hilft es ungemein beim debugging)

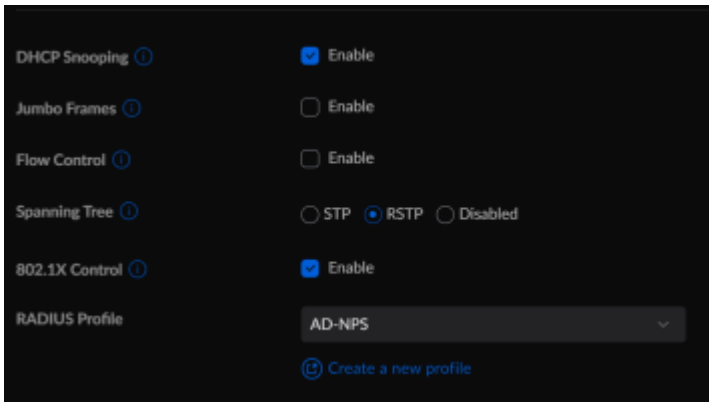
Dieselben Daten eingeben wie bei Authentication Server, mit Ausnahme vom Port, hier tragt ihr diesmal Port Nummer 1813 ein.



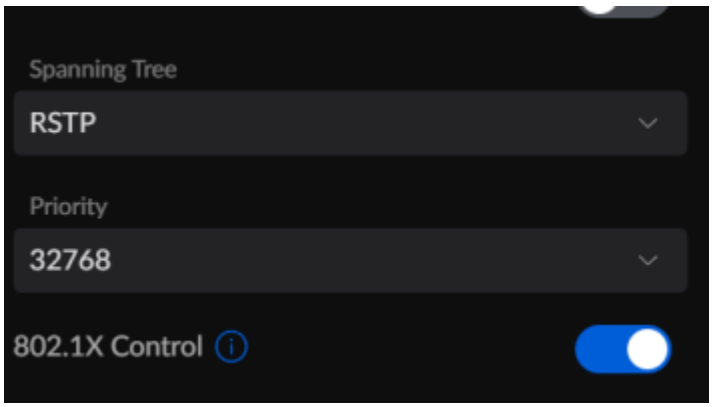
Dann geht ihr zu Netzwerk - Einstellungen - Profile - Switch Ports - Create new profile



Einstellungen - Netzwerke

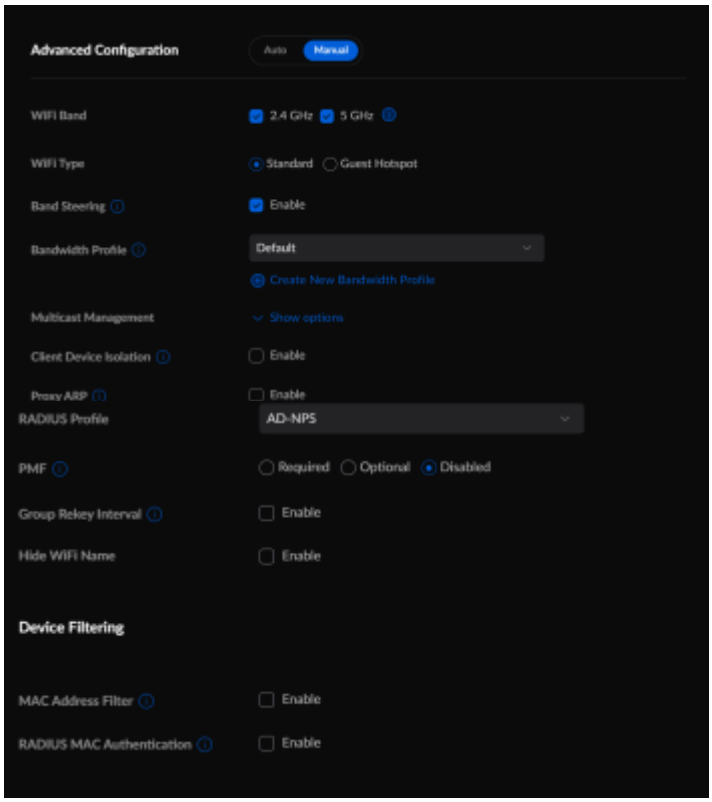


Solltet ihr einen oder mehrer Switche nicht über die globalen Netzwerk-Einstellungen verwalten, so findet ihr die nötigen Schalter unter Unifi-Devices - "euer switch" - Settings - Services



Einstellungen - WiFi

neue SSID mit Einstellungen aus dem Screenshot.



Natürlich müsst ihr noch alle Switchports, bei denen das Profil "AD-NPS" verwendet werden soll, entsprechend konfigurieren.

Unifi-Devices - "euer switch" - portmangement

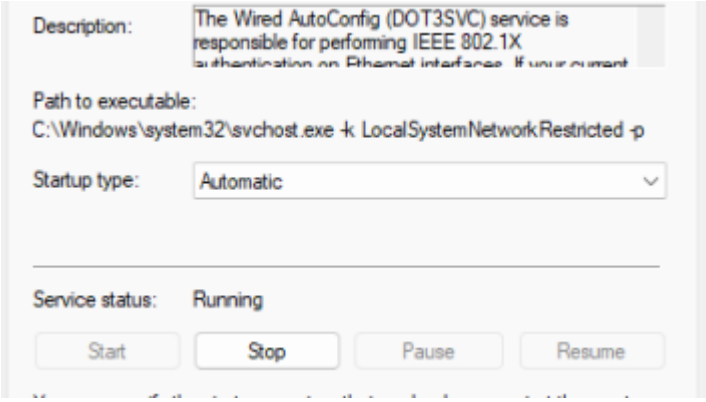
Warum auch immer muss man hier Netzwerk angeben, gleich der zweite Punkt. Es ist vollkommen egal, welches VLAN ihr hier eintragt, da es ignoriert wird. Sollte eure Authentifizierung am NPS fehlschlagen, rutschen eure Geräte automatisch in das Fallback-VLAN, das ihr bei "Global Switch Settings" eingegeben habt. Vielleicht bessert Ubiquiti hier ja irgendwann mal noch nach, damit das weniger verwirrend ist.

Das wars auch schon im Unifi-Controller.

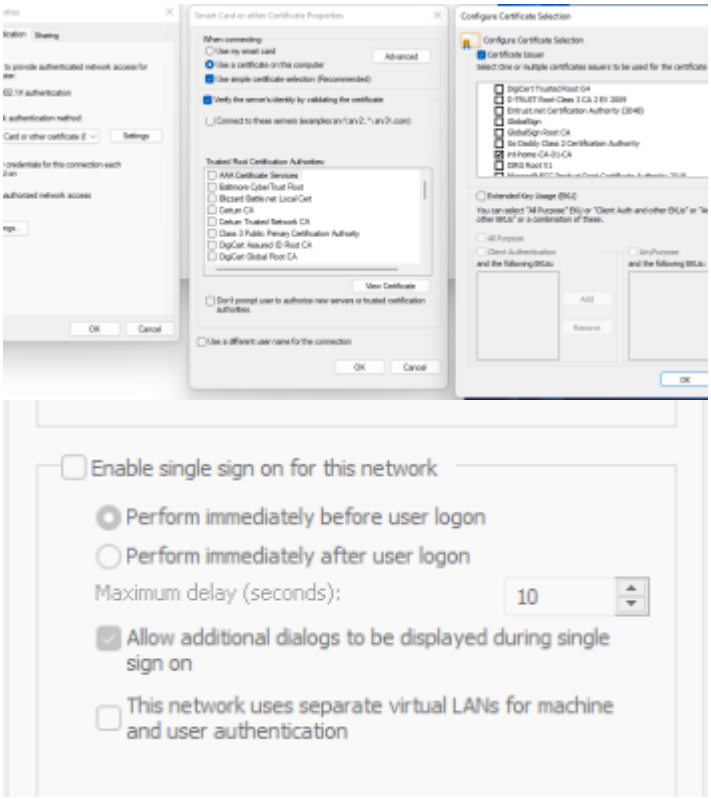
5 Lan-fähige Windows Clients konfigurieren (bei Wifi-only Clients nicht nötig)

Windows-Suche - "Dienste"

Findet den Dienst dot3svc (Wired AutoConfig, deutsch: Automatische Konfiguration (verkabelt)). Dieser muss gestartet sein und auch beim Hochfahren automatisch starten.



Wechselt nun zu den Netzwerkverbindungen. Rechtsklick auf euren Netzwerkadapter und dann Eigenschaften. Wechselt zum Reiter "Authentifizierung". Einstellungen wie in den Screenshots.



Bevor ihr scharf-schaltet, sollten alle Clients und alle Server gpupdate /force ausgeführt haben und einmal neu gestartet werden, damit auch alles GPOs übernommen wurden. Dies ist wichtig, damit die Clients die entsprechenden Zertifikatsanforderungen an die CA stellen.

6 Ergebnis

1. Nun sollten Nutzer, welche sich mit Ihrem Nutzernamen u. Passwort am WLAN anmelden in VLAN 10 eingewählt werden.

2. Der/die Nutzer der Gruppe IoT wählen sich in VLAN 16 ein

3. Laptops, die sich über WLAN verbinden und der Active Directory verbinden sich bereits vor der Nutzeranmeldung mit dem WLAN AD-Home und wählen sich im VLAN 10 ein

4. PCs, die der Active Directory angehören, werden, sobald sie mit einem Switch verbunden werden, in VLAN 10 eingewählt.

Wichtig:

für Server empfehle ich das Ganze ausdrücklich NICHT, da bei einer Fehlkonfiguration ein Aussperren aus den eigenen Systemen nicht ausgeschlossen werden kann.

Sollte ich irgendwo etwas vergessen haben zu erwähnen, nehmt es mir nicht übel, war doch alles etwas viel auf einmal zu schreiben. Weist mich einfach darauf hin, dann schau ich nochmal drüber.

Bekannte Bugs/Bugfixes:

1. Sollten eure RADIUS-Clients (Switches/Accesspoints) Schwierigkeiten haben, mit dem NPS zu kommunizieren, erstellt auf dem NPS bitte eine eingehende Firewallregel, in der ihr die Ports 1812 und 1813 erlaubt. Es besteht zwar eine solche Regel, jedoch wird sie aus welchen Gründen auch immer ignoriert. Dies ist ein bekannter Bug, der von MS auch schon bestätigt wurde.
2. Die Log-Files vom NPS lassen sich leider nicht auf einer Netzwerkfreigabe speichern. Workaround: ein Skript erstellen, welches die Dateien auf eine Freigabe synchronisiert.

Grüße aus BW und viel Erfolg beim Umsetzen!

Disclaimer:

dies ist nur eine grobe Anleitung. Ich bin weder auf diesem Gebiet geschult, noch kenne ich mich mit möglichen Sicherheitsrisiken aus. Alles was ihr tut, geschieht auf Eure eigene Verantwortung.

Auswählen:

Gültige Software-Version Keine Firmware-Relevanz!